行政院國家科學委員會專題研究計畫　成果報告

無基礎行動網路環境下身份認證與安全群播機制之研究

計畫類別：個別型計畫
計畫編號：NSC92-2416-H-009-015-
執行期間：92 年 08 月 01 日至 93 年 07 月 31 日
執行單位：國立交通大學資訊管理研究所

計畫主持人：羅濟群

計畫參與人員：黃俊傑、李秋儀、陳淑雯

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 93 年 10 月 28 日

行政院國家科學委員會專題研究計畫成果報告

無基礎行動網路環境下身份認證與安全群播機制之研究

A Study on Authentication and Secure Multicast Schemes for Mobile Ad Hoc

計畫編號：NSC 92－2416－H－009－015－

執行期限：92 年 8 月 1 日至 93 年 7 月 31 日

主持人：羅濟群　　國立交通大學資訊管理研究所

計畫參與人員：黃俊傑、李秋儀、陳淑雯　　國立交通大學資訊管理研究所

中文摘要

在無線網路中，無基礎行動網路隨著技術之演進，及克服路由與服務品質等問題後，將使得它的應用範圍更廣。由於它不需藉由無線擷取器提供服務的特性，而是可以自我組成路由環境，亦因於此，它非常適用於災難救助、軍方作戰演訓及辦公室會議環境使用。但由於它具有動態拓樸及無線網路環境所形成的弱連結現象，使得它在實際應用面所遇到的安全問題較傳統的有線網路及無線網路環境更為複雜。

在網路環境中，可藉由點對點、點對多點或多點對多點方式完成資訊傳播，但由於無基礎行動網路的特性，點對點的方式較不適用，故群播在無基礎行動網路下的應用將劇增。而身份認證與群播的安全性問題在此網路架構下完成群播之目的就顯得格外重要。另具叢集架構之無基礎行動網路環境，使得路由及金鑰管理上較有效率。因此，本研究針對在叢集架構下的無基礎行動網路環境，就身份認證及點對多點的安全群播問題做研究。本研究提出具相互認證的身份認證機制，並在群播架構下就通訊點的單一節點/多個節點加入、單一節點/多個節點離開及金匙管理問題提出較佳的安全機制與架構，以符合在無基礎行動網路中因動態拓樸與無線通訊本身之限制下，能完成安全且具有效率的群播通訊環境。最後，於安全性分析上，本機制除滿足安全性需求外，另由於每個節點所握有的金鑰數量及因更新群組金鑰所需傳送的訊息量較其他機制少，故本研究所提的機制應可提供較佳的安全性與運作效率。

關鍵字：無基礎行動網路、身份認證、安全群播、金鑰管理

Abstract

After overcomes the routing and quality of service problems, the Mobile Ad Hoc Networks, MANET, make the application in this environment more popular than before. MANET can self-organize routing and does not need access point, so it is useful for emergency operation, military environment and conference. Owing to dynamic topology and wireless environment its secure problems are more complex than wired or wireless network environments in the reality applications.

There are many ways for information dissemination during communication, but due to the characteristic of MANET the point-to-multipoint method is more applicable than others. Multicast is rapidly becoming a more application in the MANET environment. Therefore, the security problems of authentication and secure multicast are more significant, and focus these two in our research. In addition, the cluster-based MANET can get more efficient than others in the aspect of routing and key management. We will propose mutual authentication scheme and think more secure scheme and scalable architecture for multicast while some node joins or leaves from the multicast tree and key management problems in the above architecture. We make multicast more efficient and secure under the restriction of the dynamic topology and infrastructureless and wireless network constraint in MANET environment. Finally, security analysis present the schemes we proposed are more secure and efficient than the others.

Keywords: Mobile Ad-Hoc Networks, Authentication, Secure Multicast, Key Management

一、計畫緣由與目的

隨著網路環境不斷的改善，各式的通訊服務，如語音、文件、影像得以在通訊平台上傳輸資訊。其中又以無線通訊因它具有可移動性特性，使得它更加受人喜愛。目前無線通訊可分成兩種，一是有基礎架構(infrastructure)之通訊網路環境，例如藉由無線擷取器(Access point)所構成的無線區域網路環境；另一個為無基礎架構之通訊網路環境，即無基礎行動網路(Mobile Ad Hoc Network, MANET)。由於在有基礎架構之通訊環境須倚賴無線擷取器的存在方能完成資訊的轉送，因此，若有無線擷取器損毀、或因自然災害或因無線擷取器無法涵蓋的範圍，則此通訊管道失去作用，將造成節點間無法通訊。而無基礎架構之無基礎行動網路，正可解決上述問題[12] 。

無基礎行動網路特性即是節點間之通訊並不須預存一個基礎網路的設置，它們彼此間能自我組成(Self-Organization)完成構連，建立起通訊管道，而當兩個節點間已超過無線電電波範圍(radio range)，則另一個行動機即具有路由功能，以搭起此兩通訊機間通訊通道。因此，它除了具有傳統無線通訊的可移動性優點外，又因它具有無基礎架構的特性，其應用範圍更廣。

之所以要在無基礎行動網路環境下討論安全機制問題，其原因包括：

1. 無線網路本身即是一個受攻擊的通訊環境，不管是竊聽、干擾或是阻斷服務的攻擊，都會造成嚴重的影響。
2. 長期間的通訊下一些非法入侵的行為是不可避免的。
3. 無基礎行動網路它是一種無基礎架構的網路環境，因此並未具有集中式管理的特性。
4. 通訊節點隨時可能加入或移出某一個通訊區域。

從上述問題得知，在此無線通訊環境中應具有身份驗證(Authentication)、私密性(Confidentiality)、資料傳遞的正確性(Integrity)、不可否認性(Non-repudiation)及存取控制(Access control)等安全機制作為第一道防線，再加上入侵偵測以防止阻斷服務(Deny of Service, DOS)或分散式阻斷服務(Distributed Deny of Service, DDOS)的攻擊。本研究將針對身份驗證機制做更進一步探討，以期提出一個相互驗證且具有效率的身分驗證機制。另就群播之金鑰管理及節點的加入與離開所造成的安全問題做討論。另由於具有叢集架構的無基礎行動網路(Cluster-based Ad-Hoc Networks)，將使得它在一個具有很大且動態的網路中較其他架構更具有效率，故本研究是在此架構環境中討論安全性問題。由於上述安全機制的提出，使得無基礎行動網路環境更易實現。

二、文獻探討

2.1 無基礎行動網路環境

在無基礎行動網路環境中，節點間可以做直接的通訊，也能隨意移動，並繼續保持節點間連線的狀態。無基礎行動網路是由無線裝置自行建立的區域網路環境，其中並無無線擷取器或橋接器，它是一種能夠在沒有事先建置基礎架構的環境下，讓各個節點透過彼此點對點連結所構成的網路，使得節點間彼此之間能夠互相傳送資料，其架構圖如下圖 一所示。

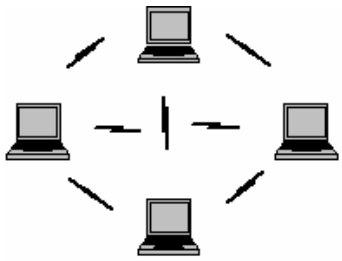

圖 一：無基礎行動網路架構

而無基礎行動網路最主要的特色包括動態拓樸及具有自我組織的能力。由於具有動態拓樸的特性使得各個連結設備可以任意移動位置，且還能繼續和其他節點做溝通；而因具有自我組織，使得一方面它不但可以簡化網路的管理，提高其強健性(robustness) 和彈性，另一方面，它更能在處於動態的狀況下，像位置移動、不定的連結、和無法預測的流量負載的既定基礎結構下，作最理想的

資源有效使用。

由於無基礎行動網路並沒有無線擷取器、路由器等之裝置，因此，每個節點除了扮演一般的使用者之外，也必須同時具備有路由器的能力。由於在無基礎行動網路環境，每個節點具有高度的動態特性，所以傳統的路由架構如 link-state 以及 distance-vector[8] [4] ，均不適用。故以下即就無基礎行動網路路由架構做說明：

1. Proactive Protocol：也稱做 table-driven protocol，這個方式會經常性的去更新路由的路徑，當有封包需要被傳送時，路由的路徑通常是可以立刻得知的，使得封包能夠即時的被傳送出去。採用 proactive 方式的協定有：Destination-Sequenced Distance Vector protocol (DSDV)[2] 、Temporally-Ordered Routing protocol (TORA) [19] 、Lightweight Mobile Routing protocol (LMR)[15] 等。Proactive 協定的好處是，當有封包需要傳送時，路由路徑能夠很快決定;但是,單純的採用 proactive 方式並不能完全適用於無基礎行動網路上，因為節點會經常性的改變位置，維持路由的資訊會佔用網路很大的資源，且可能會有某些路由資訊在過期之前，都不會被用到，而浪費了網路的資源。
2. Reactive Protocol：也稱做 on-demand protocol，這個方式只有在當有路由需求時，才會去進行路由路徑的決定。採用 reactive 方式的協定有：Ad hoc On Demand Distance Vector protocol (AODV)[1] 、Dynamic Source Routing protocol (DSR)[6] 等。由於在收到路由需求的訊息時，路由資訊可能不存在，因此，決定路由路徑將會造成封包傳送延遲時間較長，且在決定路由路徑時所需要的廣播訊息將會佔用很多頻寬，因此，單純的採用 reactive 協定也無法完全適用於無基礎行動網路上。

基於以上兩種路由協定，進而有學者提出應用於以叢集為基礎的無基礎行動網路(Cluster Based Mobile Ad-Hoc Networks)的路由協定：Cluster Based Routing Protocol (CBRP)[13] ，在這樣的架構下，由於叢集頭(cluster head)已經知道屬於它的叢集成員(cluster member)的資訊，因此，路由需要訊息的廣播只需要在叢集頭之間進行，不但能夠有效減少傳送路由訊息所需佔用的頻寬，也能較快速的決定路由路徑，這也是本研究最後選擇採用叢集式架構的原因之一。

由於一般無線網路與有線實體網路傳輸媒介的差異，加上無基礎行動網路本身具有的特性，並非所有的安全協定皆適用於無基礎行動網路環境；因此，想要在無基礎行動網路上建構安全的通訊環境必須特別注意可能面臨到的挑戰，例如於[11] 所提的相關問題，均值得探討。

基於以上的討論，在無基礎行動網路環境中，節點之間要如何傳送訊息、溝通，是一個重要的議題。因此，有許多學者提出應用於無基礎行動網路的架構[7] [5] ，大致包含以下三種：集中式架構(centralized)、階層式架構(hierarchical)及叢集架構(cluster-based) [10] [20] 。

其中叢集架構是將網路中的節點分成數個叢集，每個叢集中有各自的一個叢集頭及數個叢集成員，由叢集頭來負責成員的管理，及訊息轉送與傳送等動作。由於網路是被分成多個小叢集，因此管理網路成員將更方便；且成員的認證是由叢集頭與每個成員個別來進行，不需透過多階傳輸，減少認證過程中遭受攻擊的可能性。

叢集頭所需扮演的角色較複雜，因此需要有較強的計算能力，在動態的網路中，如何選出適合的叢集頭，並保證叢集頭不是一個非法的使用者，是無基礎行動網路的問題之一。叢集頭的選定方式大致有 Identifier-based Clustering 與 Connectivity-based Clustering 兩種[3] 。另外在叢集架構下有一個稱做閘道點(gateway node)[10] ，它是用來負責連接兩個群組之間的通訊。

基於以上路由架構與安全性的考量，本研究將採用叢集式架構，來有效達到安全的訊息傳送以及成員管理的目的。

2.2 身份認證機制

在無基礎行動網路環境中，由於節點間並不實際存在一條實體的通訊通道，而是藉由電波在空氣中傳遞資訊，任何人更容易截

聽到通訊內容，亦因於此，通訊通道的隱密性顯得更為重要。另外，由於用戶端可自由的移動，容易造成攻擊者竊聽或非法使用的情形發生。而身份認證的使用將可解決上述問題。

有關身份驗證機制 Bellovin 與 Merritt 於 1992 年首先提出運用於雙方的通行碼驗證交換協定，一般也稱之為 Encrypted Key Exchange (EKE) 協定[17] 。此協定主要目的就是為欲通訊的雙方分配一把金鑰且同時利用通行碼達到相互身份驗證(mutual authentication)。在整個協定它利用雙方事先已知的密碼 P ，並將挑戰值的關念引進，以達到雙方身份認證之目的。其提出的概念說明如下圖 二。

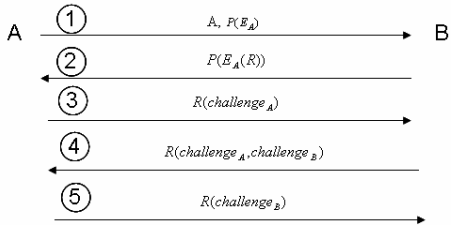

圖 二：Bellovin and Merritt Scheme

在本研究中身份認證機制是在任一節點欲加入某一叢集而成為成員之一，它必須用它與此叢集頭事先共同擁有的金鑰，經由挑戰與回應的程序，以達到相互認證之目的，最後由此叢集頭將此節點分配到的輔助金鑰藉由事先共同擁有的金鑰傳送給此新加入的節點。

2.3 安全群播機制

網路上資料的傳遞不外乎三種方式：Unicast、Broadcast 及 Multicast。其中又以 Multicast 的效率較佳。資料接收端必須指定要加入網路上任一的群播群組，因此資料發送端只要送一次資料則不論資料接收端有多少，都能讓所有加入此群組的使用者接收到資料。由於隨著網際網路與網路上通訊服務的快速成長，群體通訊變的越來越重要。群體通訊的服務包括：IP 電話、視訊會議、及協同式工作場所等等。同步、安全、及隱私對群體通訊是必要的。因此如何提供安全的群播，讓付費網路多媒體、責任性言論、公告及私人會議等群組應用，在傳送資料時能做到保密及認證的功能，是目前一項重要的研究課題。

所謂安全的群播，就是在群組成員在通訊時，必須提供溝通資料的私密性及可認證性的機制，滿足下列幾點的特性：[14]

1. 非群組成員，不能夠得知群組成員之間資料傳送的內容。
2. 成員間資料的傳送必需提供有來源端認證的機制。
3. 一個新加入的成員，不能夠得知他加入群組之前，群組成員間資料傳送的內容。
4. 一個離開群組的成員，不能得知其離開群組後，群組成員間資料傳送的內容。

要達到上述四點的安全群播特性，必需在群組成員間建立一個共享的加解密金匙，並作安全且有效率的管理。在[22] 一文中即對安全群播作詳盡的描述，以下摘其內容做說明：『一般安全群播協定需建立一群播金匙的管理機制(Key Management)，使得加解密金匙的共享不限定於兩者之間，而是由群組成員所共享，通常這把加解密金匙被稱為群組金鑰(Group Key，簡稱 GrpKey)』，另藉由輔助金鑰達到群組金鑰更新的目的。

一般而言，群組金鑰管理方法可分成三類[18] ：(1)集中式的金鑰管理：由單一個金鑰分佈中心或管理者來產生群組金鑰。(2)半集中式的金鑰管理：將整個群組分成多個子群組，並由各子群組管理者來產生金鑰。(3)分散式的金鑰管理：沒有單一個金鑰分佈中心，群組金鑰的建立是每個成員貢獻其密秘值且成員間彼此合作之下而建立的；一般又將前二種類型稱為金鑰分佈協定(key distribution protocol)，而將第三種類型則稱為金鑰協同協定(key agreement protocol)。

由於本研究採叢集式的拓樸協定，因此於安全群播之金鑰管理協定將以半集中式的方式達到安全群播的效果。本研究之安全群播機制基於[9] 作者所提的 EBS（Exclusive Basis Systems）並結合 sum of product 的觀念應用於叢集內與叢集間的金鑰管理與動態成員加入與離開，使其達到安全群播之效果。以下即就 EBS 機制做完整性介紹。

在[9] 之文獻中，提及當群體的成員經常

變動時，如何能有效率管理群播的群體密鑰的方法。此方法稱之為 EBS，它改善了目前以二元樹為基礎及其他相關系統的密鑰管理方法。

在群體中，每位成員不僅握有群體密鑰，還個別握有數把用來協助群體密鑰更新的輔助金匙。這篇論文提出一個技術，稱為 EBS，此為一個群體密鑰管理的組合公式，即如何在成員數為 n 下，求出最佳的 k 和 m。n 指的是群體成員數，k 則為每個成員握有的輔助金匙數，m 是每次更新群體密鑰所需送出的訊息數。在這篇論文中，描述了單一成員加入離開的演算法，並且驗證了大型群體採用 EBS 進行密鑰管理的效率。

EBS 定義：令 n、k、m 皆為正整數，$1 < k、m < n$。我們將 EBS(n, k, m)表示為數個子集(內容為$[1, n] = \{1, 2, \ldots, n\}$)的集合體，令它為 Γ。每個整數 $t \in [1, n]$滿足以下兩個特性：

1.t 最多只能出現在 Γ 中的 k 個子集合。

2. 在 Γ 中，會有 m 個子集合，即 $A_1, A_2, \ldots, A_m$，使得$\bigcup_{i=1}^{m} A_i = [1, n]-\{t\}$(表示若要排除掉 t 元素，需要 m 個在 Γ 中的子集合做聯集)。

舉例如下：EBS(8, 3, 2)是一個數個子集合的集合體 $\Gamma = \{A_1=\{5, 6, 7, 8\}, A_2=\{2, 3, 4, 8\}, A_3=\{1, 3, 4, 6, 7\}, A_4=\{1, 2, 4, 5, 7\}, A_5=\{1, 2, 3, 5, 6, 8\}\}$。我們可以簡易的驗證每個 $t \in [1, 8]$在 Γ 所有子集合中僅出現 3 次，且每個成員都被在 Γ 中的兩個子集合聯集後排除。就像下面圖 三所示：

$$[1,8]-\{1\} = A_1 \cup A_2$$
$$[1,8]-\{2\} = A_1 \cup A_3$$
$$[1,8]-\{3\} = A_1 \cup A_4$$
$$[1,8]-\{4\} = A_1 \cup A_5$$
$$[1,8]-\{5\} = A_2 \cup A_3$$
$$[1,8]-\{6\} = A_2 \cup A_4$$
$$[1,8]-\{7\} = A_2 \cup A_5$$
$$[1,8]-\{8\} = A_3 \cup A_4$$

圖 三：扣除某一成員之表示法

一個維度為(n, k, m)的 EBS 集合體 Γ，表示在群體中有編號為 1 到 n 的 n 個使用者，而密鑰伺服器（Key Server）保管集合體 Γ 中所有子集合的輔助金匙（即為 A_i）。若 A_i 出現在 Γ 中，表示出現在 A_i 此子集合中的所有成員都握有這把輔助金匙，像上例 EBS(8, 3, 2)中，僅有成員 5、6、7、8 才握有輔助金匙 A_1。而對於$\bigcup_{i=1}^{m} A_i = [1, n]-\{t\}$此特性，即表示當密鑰伺服器想驅逐某位成員時，可以使用$\bigcup_{i=1}^{m} A_i$ 中所有的 A_i 來加密新的群體密鑰送給留下來的成員，換句話說，當有成員離開群體，密鑰伺服器僅需群播出 m 個用$\bigcup_{i=1}^{m} A_i$ 中所有 A_i 加密過的訊息給所有群體成員，如此可確保除了 t 以外的所有成員都可獲得新的群體密鑰。

當有成員離開時，除了更新群體密鑰，該成員握有的輔助金匙亦需更新以避免串謀攻擊，此論文建議可採用雜湊函數 f(新群體密鑰, 舊 A_i)來算出新的 A_i，如此不但可確保僅原先握有該輔助金匙者才可得出新的 A_i，亦可避免由密鑰伺服器產生新 A_i 後，以舊 A_i 加密後再傳送給所有成員的流量浪費。

首先我們先列舉如何在 k+m 個物件中，形成 k 個子集合的可能方法。對於所有的 k 和 m，我們令 Canonical(k, m)為$\binom{k+m}{k}$以在 k+m 個物件中，形成 k 個子集合。舉例矩陣 A=$\binom{5}{3}$，如圖 四所示：

0	0	1	0	1	1	0	1	1	1
0	1	0	1	0	1	1	0	1	1
1	0	0	1	1	0	1	1	0	1
1	1	1	0	0	0	1	1	1	0
1	1	1	1	1	1	0	0	0	0

圖 四：子集合 A_i 與成員間關係

此矩陣即可用來管理當群體成員為 10 時的輔助金匙分配表。在此例中，n=10，k=3，m=2。因此當有某位成員要離開時，僅需以 m=2 兩個 A_i 加密送出 rekey 訊息即可。假設成員 1 離開此群體，僅需以 A_1（握有 A_1 者包含 M3、M5、M6、M8、M9、M10）和 A_2（握有 A_2 者包含 M2、M4、M6、M7、M9、M10)分別加密新群體密鑰後送出，則除了成員 1 以外的所有其他成員都能解開此訊息。需注

意的是$\binom{k+m}{k}$必須大於 n，亦即每位成員握有的 Key String 都不相同，如此才可確保此密鑰管理系統的安全性。

當新成員加入一個群體大小為 n 的群體時，若$\binom{k+m}{k}$仍大於或等於 n+1，則僅需分配新的 Key String 和對應的輔助金匙給該成員。反之，若$\binom{k+m}{k}$小於 n+1，則可採用兩種方法：增加每個人握有的輔助金匙數或是增加 rekey 訊息的送出次數。

當成員離開時，關於 rekey 的運作，即採用上述聯集所產生的輔助金匙，來加密新的群體密鑰送出，確保離開的成員無法解開。但除了 rekey 的部分，我們仍須考量如何減少密鑰伺服器所管理的輔助金匙數，每位成員握有的輔助金匙數，以及 rekey 訊息送出的次數。

因此當新成員離開一個群體大小為 n 的群體時，若可以較少的 k 或 m 滿足$\binom{k+m}{k}$仍大於或等於 n-1，則需減少每位成員握有的輔助金匙數或 rekey 訊息送出的次數，以達到 EBS 的最佳化。

若離開成員 y 即是最後加入者，只需將系統回復到 y 加入前的狀態即可（及回復到先前所採用的 k 及 m 個數）。但當離開成員和最後加入成員的對象不同時，採用以下運作方式：

當成員 x 要離開此群體，而成員 y 是最後加入者，則：

1. 將 x 和 y 驅逐出此群體（x 和 y 握有的 A_i 都會在 rekey 的訊息中被更新）。
2. 增加成員 y 回此群體。
3. 但成員 y 會被分配先前成員 x 的 Key String 和新的對應 A_i。

EBS 在密鑰管理方法上提供一個新的架構，且 EBS 所需採用的輔助金匙個數和 rekey 訊息送出次數，都明顯優於以二元樹資料結構來管理輔助金匙。另外，由於本研究僅就金鑰管理與單人加入/離開問題做討論，並未說明如何有效做安全群播與多人離開之機制研究，因此，本研究除了將 EBS 方法引至無基礎行動網路環境，並結合 sum of product 概念達到上述效果。

三、研究方法

本研究是基植於叢集架構下的無基礎行動網路環境下，將具有相互認證的身份認證機制及安全群播機制加入，以達到從初始階段至群組金鑰更新階段，都能滿足安全性的需求。以下即就本研究之機制與安全性分析做描述。

3.1 本研究之無基礎行動網路架構

本研究乃基於叢集架構下討論無基礎行動網路的身份認證與安全群播兩個安全議題。因此，它包括了叢集內與叢集間的身份認證與動態環境下的金鑰管理機制，以滿足安全群播之目標。而之所以採用叢集架構，其原因為它具有較佳的路由效率。因此，在本研究中我們假設和叢集頭能直接進行通訊(Single Hop)的所有成員為一個叢集，在叢集內的成員共同分享一把子群組金鑰。不同叢集間亦可透過叢集頭，使用 Inter-cluster key 互相通訊。而任何一個節點均可加入或離開某一叢集。在本研究機制中是以編號最小者做為該叢集之叢集頭，且此叢集頭具有可信賴的特性，除非此叢集頭離開了此叢集，則必須重新找叢集頭，且重建此叢集內所有成員的信賴關係，且該叢集頭必須重新取得叢集間的群組通訊金鑰及輔助金鑰。於叢集間亦以編號最小的叢集之叢集頭當做此群組之叢集頭。同樣的，它必須具備與叢集內之叢集頭同樣的特性，它的目的是為了實現跨叢集的安全群播。下圖 五即為本研究之叢集架構圖。

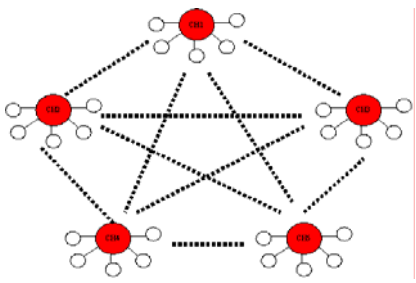

圖 五：叢集架構之無基礎行動網路

另先就本研究所須之假設在此做描述：

假設 1：

此群組通訊環境共區分成 n 個叢集，即 $GS = \{CH_i \mid \forall i = 0,...,n-1\}$ ；每個叢集擁有 m 個成員(節點)，即 $CH_i = \{M_{i,j} \mid j = 0,1,2...\}$ ，其中每個叢集內的成員個數可以不一樣。

假設 2：

$M_{0,0}$ 為此群組通訊主要控制者，由它來產生叢集間的群組金鑰及各叢集頭的輔助金鑰，做為叢集間更換群組金鑰之用；而 $M_{i,0}$ 為第 *i+1* 個叢集之叢集頭，其目的是為了產生此叢集之子群組金鑰及該叢集內所有成員的輔助金鑰，做為叢集內更換子群組金鑰之用。另所有叢集之叢集頭均為可信賴的節點，由它們來協助完成金鑰管理與群播工作。

假設 3：

$M_{0,0}$ 與 $M_{i,0}; \forall i = 1,2,...,n-1$ 間已存在一個密祕金鑰 PW_i ；同理每一個叢集頭 $M_{i,0}$ 與該叢集內的所有成員 $M_{i,j}; j = 1,2,...$ ，亦存在一個密秘金鑰 SPW_j 。

假設 4：

叢集內之叢集頭 $M_{i,0}$ 或此通訊群組之叢集頭 $M_{0,0}$ 必須協助合法的群組成員完成群播事宜。

3.2 身份認證機制

於身份認證機制上，它是應用於初始階段。包括叢集內所有節點與該叢集頭的相互身份認證，只有通過認證的節點，該叢集頭才會分配給該節點參加此叢集所必需的輔助金鑰；及叢集與叢集間相互認證機制。以下即就此身份認證機制做細部描述。

1.叢集間的身份認證機制($M_{0,0} \leftrightarrow M_{i,0}$)

本研究所提的身份認證機制具有相互認證功能，並藉由挑戰與回應的三個回合方式完成，其目的是為了防止重送及 Man-in-the-middle 攻擊，下圖 六為本認證機制之協定。

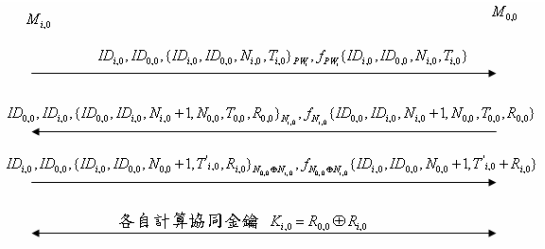

圖 六：叢集間身份認證機制

由於本協定之單向雜湊函數具有金鑰，因此，更具有確認資料來源端身份之功能，因為可以確定此單向雜湊函數是由此 $M_{i,0}$ 產生，而非其它節點產生，以防止 Man-in-the-middle 攻擊。另 T 為時間戳記，N 與 R 為等同長度的隨機亂數；T 與 N 的目的是為了防止重送攻擊。另第二、三回合之所以要用不同的金鑰加密，其原因為主金鑰不應出現於所有回合中，以防止有可能的密碼猜猜測攻擊，另一方面藉此實現對稱密碼系統的一次使用原則，以加強密碼系統的強度。最後，協同金鑰產生的目的是為了讓後續進行群播時，若此叢集頭 $M_{i,0}$ 須請 $M_{0,0}$ 協助完成群播時加密該訊息內容之用。

2. 叢集內的身份認證機制($M_{i,0} \leftrightarrow M_{i,j}$)

叢集內的身份認證機制，其目的是為了某一節點能順利的加入某一叢集，進而為該節點產生子群組金鑰與輔助金鑰，作為群播之用與未來更新子群組金鑰之用。叢集內的身份認證機制與叢集間的身份認證機制做法一致，下圖 七為本認證機制之協定。

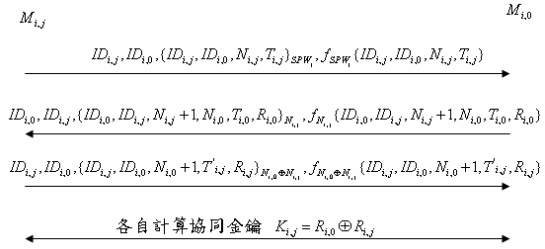

圖 七：叢集內身份認證機制

因此，對某一節點欲加入某一叢集，或某一新增叢集欲加入至此群組通訊，待完成上述具相互認證之身份認證機制，即完成初始階段。下一階段為群組金鑰、群組輔助金鑰、子群組金鑰及子群組輔助金鑰之產生與管理。

3.3 安全群播與金鑰管理

由於群播具有點對多點遞送之效果，故非常適用於無基礎行動網路環境。本小節就群播金鑰之管理，做詳細介紹。

本機制採[9] 所提之 EBS 機制，並使用 sum of product 的機制以達快速化簡之目的，如此使得群播所需之輔助金鑰及當有成員離開群組，完成更新此群組金鑰之後，將新的群組金鑰送至現有成員所需使用之輔助金鑰能很快的計算出來。於本研究中，安全群播之金鑰管理，亦區分叢集間與叢集內之金鑰管理機制。亦即是說，對某一叢集而言，該叢集頭必須協助通過的節點產生子群組金鑰及子群組輔助金鑰，作為該叢集內任一節點欲進行叢集內群播之用；另對叢集間而言，$M_{0,0}$ 必須協助剛加入此通訊群組之叢集代表，即是該叢集之叢集頭 $M_{i,0}$ 產生輔助金鑰及該群組之群組金鑰。因此，該叢集頭即可協助該叢集之成員完成跨叢集群播之目的。以下即就每一種情況做描述。

1.叢集內群播與金鑰管理機制

某一節點通過身份認證後，叢集頭必須有義務協助它成為叢集的成員之一。因此，就叢集頭而言，它必須執行 EBS 之成員加入機制。而當某一成員欲進行群播時，其步驟如下：

a. $M_{i,j}$ 必須決定群播對象有哪些。

b. $M_{i,j}$ 將此群播的訊息藉由先前已於認證階段所產生的共同金鑰 $K_{i,j}$ ，使用對稱式密碼系統加密，並傳送至此叢集頭 $M_{i,0}$ 。此 $M_{i,j}$ 所需加密與傳送的內容，包括訊息 M，群播對象的 ID，及若需要更換共同金鑰 $K_{i,j}$ 時可將新的 $R_{i,j}$ 送至叢集頭。如此，此節點待拿到叢集頭給的新 $R_{i,0}$ ，即可重新產生新的共同金鑰 $K'_{i,j}$ 。因此，更能確保通訊的保密性。

c. 叢集頭 $M_{i,0}$ 解開訊息後，便依據 $M_{i,j}$ 所要求的群播對象進行群播。此時 $M_{i,0}$ 會先藉由 sum of product 算出最後須由哪幾把子群組輔助金鑰須相互合作，以達訊息群播之目的。另外，它會檢查是否需要重新產生新的 $R_{i,0}$ 給該節點，以更新它與此節點的共同金鑰 $K'_{i,j} = R'_{i,0} \oplus R'_{i,j}$ 。

d.任一節點收到此群播訊息後，由於它是屬於合法的接收成員，故可用它手中的子群組輔助金鑰進行組合以解開此訊息。

若有某一成員或某一群成員離開此叢集時，叢集頭除了必須依照 EBS 演算法驅離此叢集內需離開的成員外，亦須藉由 sum of product 化簡機制將新的子群組金鑰藉由此化簡後結果的子群組輔助金鑰之組合送至未離開的節點手中。最後，再將不應該驅離的成員加回到此叢集。以上即是叢集內群播與金鑰管理機制。

2.叢集間群播與金鑰管理機制

某一個新加入的叢集 CH_i 通過身份認證後，叢集頭 $M_{0,0}$ 必須協助此叢集之叢集頭 $M_{i,0}$ 成為群組成員之一，如此此叢集頭 $M_{i,0}$ 才有能力產生叢集內通訊所需子群組金鑰及協助新加入該叢集的節點產生子群組輔助金鑰。因此，就叢集頭 $M_{0,0}$ 而言，它必須執行 EBS 之成員加入機制。而當某一叢集頭 $M_{i,0}$ 欲進行群播時，其作法與叢集內做法相似，步驟如下：

a. $M_{i,0}$ 必須決定群播對象有哪些。

b. $M_{i,0}$ 將此群播的訊息藉由先前已於認證階段所產生的共同金鑰 $K_{i,0}$ ，使用對稱式密碼系統加密，並傳送至此叢集頭 $M_{0,0}$ 。此 $M_{i,0}$ 所需加密與傳送的內容，包括訊息 M，群播對象的 ID，及若需要更換共同金鑰 $K_{i,0}$ 時可將新的 $R_{i,0}$ 送至叢集頭。如此，此叢集頭 $M_{i,0}$ 待拿到叢集頭 $M_{0,0}$ 給的新 $R_{0,0}$ ，即可產生新的共同金鑰 $K'_{i,0}$ 。因此，更能確保通訊的保密性。

c.叢集頭 $M_{0,0}$ 解開訊息後，便依據 $M_{i,0}$ 所要求的群播對象進行群播。此時 $M_{0,0}$ 會先藉由 sum of product 算出最後須由哪幾把群組輔助金鑰須相互合

作，以達訊息群播之目的。另外，它會檢查是否需要重新產生新的$R_{0,0}$給該節點，以更新它與此節點的共同金鑰$K'_{i,0} = R'_{0,0} \oplus R'_{i,0}$。

d.任一叢集頭收到群播訊息後，由於它是屬於合法的接收成員，故可用它手中的輔助金鑰進行組合以解開此訊息。

若有某一叢集頭或某一群叢集頭離開此通訊群組時，受影響到的那些叢集必須重建叢集。亦即是說，某一叢集頭的離開，可能導致該叢集須重新找到一個新的叢集頭作為此叢集子群組金鑰與子群組輔助金鑰的產生者與管理者；或是可能原先一個叢集備分割成多個叢集亦有可能，在此情況，仍依上述做法為每個新的叢集找出叢集頭。對所有新產生的叢集頭，他們必須先與$M_{0,0}$進行身份驗證機制，以便獲得群組金鑰與群組輔助金鑰。

而對叢集頭$M_{0,0}$而言，除必須依EBS演算法驅離此叢集內需離開的成員外，亦須藉由sum of product化簡機制將新的群組金鑰藉由此化簡後結果的群組輔助金鑰之組合送至未離開的節點手中。最後，再將不應該驅離的叢集頭加回到此通訊群組。以上即是叢集間群播與金鑰管理機制。

3.叢集內與叢集間混合之安全群播機制

假設某一叢集CH_i之某一節點$M_{i,j}$欲執行跨叢集的群播，此時的群播機制做法如下：

a.$M_{i,j}$必須決定群播對象有哪些。

b.$M_{i,j}$ 將此群播的訊息藉由先前已於認證階段所產生的共同金鑰$K_{i,0}$，使用對稱式密碼系統加密，並傳送至此叢集頭$M_{i,0}$。此節點$M_{i,j}$所需加密與傳送的內容，包括訊息M，群播對象的所有節點之ID及其相對應叢集ID，及若需要更換共同金鑰$K_{i,j}$時可將新的$R_{i,j}$送至叢集頭。如此，此節點$M_{i,j}$待拿到叢集頭$M_{i,0}$給的新$R_{i,0}$，即可產生新的共同金鑰$K'_{i,j}$。因此，更能確保通訊的保密性。

c. 叢集頭$M_{i,0}$解開訊息後，便依據$M_{i,j}$所要求的群播對象轉成自己的需求，並重複叢集間的群播機制。另外，它會檢查是否需要重新產生新的$R_{i,0}$給該節點，以更新它與此節點的共同金鑰$K'_{i,j} = R'_{i,0} \oplus R'_{i,j}$。

d.叢集頭$M_{0,0}$解開訊息後，它會依照訊息內容藉由sum of product化簡機制找出符合的輔助金鑰，將此群播訊息轉至那些節點所屬的叢集之叢集頭手中。任一叢集頭收到此群播訊息後，由於它是屬於合法的接收成員，故可用它手中的輔助金鑰進行組合以解開此訊息，然後再利用叢集內的群播機制送到必須收到此群播訊息的成員手中。以上即是叢集內與叢集間混合之安全群播機制。

3.4 安全性分析

本小節將就本研究所提的具相互認證的身份認證機制及安全群播機制做安全性分析。其中於身份認證機制上經驗證可抵擋重送、Man-in-middle 及密碼猜測之攻擊。另於安全群播機制上探討是否滿足[21] 作者所提的安全性條件。其條件包括群組金鑰安全、金鑰獨立性、前推安全性(Forward Security)、後推安全性 (Backward Security)，經驗證亦滿足上述要求。

另於執行效率上，由於本研究採EBS為本研究之根基，故於回合數、訊息量上較其他架構來的有效率。另本研究將 sum of product的觀念與EBS結合，使得它在群播上及應用於單一節點或多個節點同時離開能很快的將子群組金鑰分配到未離開此叢集之群組成員手中。

四、結論與建議

無基礎行動網路因具有動態拓樸即自我組織之特性，使得它有別於其他無線網路架構，故使得它可應用的範圍更廣。而通訊過程的私密性、資料完整性、身份驗證及群播機制下的金鑰管理均是無基礎行動網路所需具備的安全機制。本研究在基於叢集架構下結合半集中式的金鑰管理機制，期間將具相

互認證的身份認證機制應用於初始階段，使其只有合法且為該節點者才能獲得輔助金鑰，進而完成後續的金鑰管理協定，如此，才能藉由 EBS 結合 sum of product，找出群播金鑰，最後才能完成安全群播。

由於無基礎網路除具有無線網路的特性外，又加上本身的特質，使得它在安全機制的設計上需做改良，建議未來其他相關的安全議題，例如阻斷攻擊、存取控制等進行研究，如此，可提升該網路架構於應用上的安全性。

五、計畫成果自評

本計畫在基於叢集架構下之無基礎行動網路環境下共完成(1)具相互認證之身份機制(2)安全群播與金鑰管理機制，以上兩項均滿足本計畫之目標。由於具有相互認證之身份機制使得於初始階段只有合法且確定是該節點才能獲得輔助金匙，以便能進行後續的群播機制。而於群播的金鑰管理上，它可以使每個節點所握有的輔助金匙較少，另於群組金鑰更新階段所需傳送的訊息較少，且滿足安全群播所需之條件，故本研究機制具有後續研究價值。

參考文獻

[1] C.E. Perkins, E.M. Royer and S.R. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF MANET Working Group, Internet-Draft (March 2000).

[2] C.E. Perkins, P. Bhagwat, "Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers," in: Proc. Of ACM SIGCOMM'94, London, UK (August–September 1994) pp. 234–244.

[3] D. H. Tim, "The Cluster-Based Routing Protocol," project group 'Mobile Ad-Hoc Networks Based on Wireless LAN' winter semester 2003/2004.

[4] G.S. Malkin, M.E. Steenstrup, "Distance-vector routing, in: Routing in Communications Networks," ed. M.E. Steenstrup (Prentice Hall, 1995).

[5] H. Luo and S. Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks," Technical Report TR-200030, Dept. of Computer Science, UCLA, 2000.

[6] J. Broch, D.B. Johnson and D.A. Maltz, "The dynamic source routing protocol for mobile ad hoc networks," IETF MANET Working Group, Internet-Draft (October 1999).

[7] J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," IEEE 9th International Conference on Network Protocols (ICNP'01), 2001.

[8] J. Moy, "Link-state routing, in: Routing in Communications Networks," ed. M.E. Steenstrup (Prentice Hall, 1995).

[9] L. Morales, I.H. Sudborough, M. Eltoweissy and M. H. Heydari, "Combinatorial Optimization of Multicast Key Management," proceedings of the 36th Hawali International Conference on System Sciences (HICSS'03), 2002.

[10] L. Venkatraman and D. Agrawal, "A novel authentication scheme for ad hoc networks," in IEEE Wireless Communications and Networking Conference (WCNC 2000), vol. 3, pp. 1268--1273, 2000.

[11] L. Zhou and Z. Haas, "Securing Ad Hoc Networks," IEEE Network , pp.24-30, Dec, 1999.

[12] M. Conti and S. Giordano, "Mobile Ad-hoc Networking," In Proceedings of the 34th Hawail International Conference on System Sciences, 2001.

[13] M. Jiang, J. Li and Y.C. Tay, "Cluster based routing protocol (CBRP)," IETF MANET Working Group, Internet-Draft (August 1999).

[14] M. J. Moyer, J. R. Rao and P. Rohatgi, "A Survey of Security Issues in Multicast Communications," IEEE Network 13(6), Nov/Dec 1999, p.12-p.23.

[15] M.S. Corson, A. Ephremides, "A distributed routing algorithm for mobile wireless networks," Wireless Networks 1 (1995) 61–81.

[16] M.S. Corson, J. P. Macker and G. H. Cirincione, "Internet-Based Mobile Ad Hoc Networking," IEEE Internet Computing, July-August 1999, p.63-p.70.

[17] S. M. Bellovin and M. Merrit, "Encrypted key exchange: password-based protocols secure against dictionary attacks," IEEE Symposium on Research in Security and Privacy, pp.72-84, 1992.

[18] S. Rafeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," In ACM Computing Surveys, Vol.35, No.3, pp.309-329, September 2003.

[19] V.D. Park, M.S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in: Proc. of IEEE INFOCOM'97, Kobe, Japan (April 1997) pp. 1405–1413.

[20] V. Varadharajan, R. Shankaran and M. Hitchens. "Security for cluster based ad hoc networks," Computer Communications, 27(2004): 488-501.

[21] Y. Kim , A. Perrig and G. Tsudik, "Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups," In ACM CCS'00, pp.235-244, 2000.

[22] 陳惠淳，伍麗樵，"二階式群播金匙管理" ，TANET'2000, 2000, p.24-p.31.

[23] 黃永鑫， "一個用於 Ad Hoc 無線網路上的改良式金鑰協同協定"，國立交通大學資訊管理研究所碩士論文，民 93 年。